Національний університет водного господарства та природокористування
Навчально-науковий інститут автоматики, кібернетики та обчислювальної техніки

ЗАТВЕРДЖУЮ

Голова науково-методичної ради НУВГП
_____ Олег ЛАГОДНЮК

«___» _____2021

04-05-25S

СИЛАБУС навчальної дисципліни		**SYLLABUS**
Безпека інформаційних систем та захист інформації		**Information systems security and information protection**
Шифр за ОП	**13**	Code in Educational Program
Освітній рівень: бакалаврський (перший)		Educational level: Bachelor's (first)
Галузь знань: **Інформаційні технології**	**12**	Field of knowledge: **Information technologies**
Спеціальність: **Інформаційні системи та технології**	**126**	Field of study: **Information systems and technologies**
Освітня програма: **Інформаційні системи та технології**		Educational Program: **Information systems and technologies**

Силабус навчальної дисципліни Безпека інформаційних систем та захист інформації для здобувачів вищої освіти ступеня «бакалавр», які навчаються за освітньо-професійною програмою «Інформаційні системи та технології» спеціальності 126 «Інформаційні системи та технології». Рівне. НУВГП. 2020. 21 стор.

ОПП на сайті університету:
http://ep3.nuwm.edu.ua/18547/1/2017_opp_126_ict_bacalavr.pdf

Розробник силабусу: Назарук Віталій Дмитрович, канд. техн. наук, старший викладач кафедри обчислювальної техніки

Силабус схвалений на засіданні кафедри
Протокол № 6 від 23 грудня 2020 р.
Завідувач кафедри: Грицюк П. М., д-р екон. наук, професор.

Керівник ОП Турбал Ю.В., д-р техн. наук, доцент

Схвалено науково-методичною радою з якості ННІ АКОТ
Протокол № 4 від “ 11 ” лютого 2021 року

Голова науково-методичної
ради з якості ННІ: Мартинюк П. М.,д-р техн., професор

СЗ №-730 в ЕДО

ЗАГАЛЬНА ІНФОРМАЦІЯ*	
Ступінь вищої освіти	бакалавр
Освітня програма	Інформаційні системи і технології
Спеціальність	126 «Інформаційні системи і технології»
Рік навчання, семестр	4-й рік навчання, 2-й семестр
Кількість кредитів	6,0
Лекції:	26 год.
Лабораторні заняття:	26 год.
Самостійна робота:	128 год.
Курсова робота:	
Форма навчання	*денна*
Форма підсумкового контролю	екзамен
Мова викладання	українська
ІНФОРМАЦІЯ ПРО ВИКЛАДАЧА*	
ПРОФАЙЛ ЛЕКТОРА	
Лектор 	**Назарук Віталій Дмитрович**, канд. техн. наук, старший викладач кафедри обчислювальної техніки v.d.nazaruk@nuwm.edu.ua
Вікіситет	*http://wiki.nuwm.edu.ua/index.php/%D0%9D%D0%B0%D0%B7%D0%B0%D1%80%D1%83%D0%BA_%D0%92%D1%96%D1%82%D0%B0%D0%BB%D1%96%D0%B9_%D0%94%D0%BC%D0%B8%D1%82%D1%80%D0%BE%D0%B2%D0%B8%D1%87*
Як комунікувати	https://exam.nuwm.edu.ua/course/view.php?id=3019 Кафедра обчислювальної техніки: каб. 128, e-mail: kaf-ot@nuwm.edu.ua https://nuwm.edu.ua/nni-akot/kaf-ot Електроний журнал: http://desk.nuwm.edu.ua/ Розклад занять: http://desk.nuwm.edu.ua/cgi-bin/timetable.cgi Консультації (дистанційно) на платформі Google (Hangouts) Meet: https://meet.google.com/ajg-cokm-mcv?authuser=0

ПРО ДИСЦИПЛІНУ	
Анотація навчальної дисципліни, в т.ч. мета та цілі	Навчальна дисципліна «Безпека інформаційних систем та захист інформації» входить до циклу загальної підготовки студентів-бакалаврів зі спеціальності "Інформаційні системи та технології" і є однією з ключових складових фундаментальної підготовки фахівців в галузі інформаційних технологій. Навчальний курс призначений для вивчення основних засобів та заходів захисту інформації в інформаційних системах, в якому класифіковано загрози для інформації за критеріями цілісності, конфіденційності та доступності, методів та засобів їх локалізації та блокування. Подано основні принципи формування систем технічного та криптографічного захисту інформації. Надано описи та розглянуто принципи дії сучасних криптоалгоритмів, засобів хешування, генерації та технологій електронного цифрового підпису. ***Мета дисципліни*** полягає в отриманні здобувачами вищої освіти теоретичних знань та практичних навичок побудови захищених інформаційних систем на основі сучасних засобів технічного та криптографічного захисту інформації. ***Основними завданнями*** є формування системного підходу до побудови захищених інформаційних систем, набуття навиків блокування технічних каналів витоку інформації, отримання знань порядку застосування методів захисту від несанкціонованого доступу
Посилання на розміщення навчальної дисципліни на навчальній платформі Moodle	https://exam.nuwm.edu.ua/course/view.php?id=3019
Компетентності	**ЗК-2.** Здатність застосовувати знання та розуміння предметної області у практичних ситуаціях, виявляти, ставити та вирішувати проблеми. **ЗК-5.** Здатність до пошуку, оброблення та аналізу інформації з різних джерел, до використання інформаційних і комунікаційних технологій.

	ЗК-10. Навички здійснення безпечної діяльності.
Програмні результати навчання	**РН-10.** Знати відмінності та спільні риси методів керування і планування проектами, Застосовувати моделі та методи оцінки надійності програмних систем. **РН-17.** Оволодіти добрими робочими навичками працювати самостійно, або в групі, проявляючи навички лідерства, уміння отримати результат у рамках обмеженого часу з наголосом на професійну сумлінність та унеможливлення плагіату. **РН-23.** Демонструвати поєднання різних методів проектування, програмування та створення сучасних систем обробки інформації, обчислювальних систем різного призначення.
Перелік соціальних, «м'яких» навичок (soft skills)	– Уміння планувати робочий час для виконання самостійної роботи, опрацювання літератури та пошуку необхідної інформації. – Здатність комунікувати, зрозуміло та аргументовано доносити свою точку зору. – Бажання постійно навчатись, освоювати нові технології, виробляти потребу в отриманні нових знань. – Вміння працювати в команді на спільний результаь. – Здатність до критичного мислення при обговорення матеріалів навчання, перевірки результатів лабораторних робіт.

Структура навчальної дисципліни		
Лекції: 26 год.	Лабораторні роботи: 26 год.	Самостійна робота: 128 год.
Результати навчання:		
РН1. Освоїти технічні характеристики інформації, знати загрози для інформації, орієнтуватись в основних методах та засобах технічних видів розвідки		
Види навчальної роботи студента	Вивчення лекційного матеріалу (тема 1); самостійна робота з літературою; підготовка до контрольних заходів	
Методи та технології	Словесний метод; діалогічний метод; наочний метод; практичний метод; неімітаційні та імітаційні (неігрові)	

навчання	технології; інтерактивні технології (контекстне навчання; навчання на основі досвіду).
Засоби навчання	Комп'ютерна техніка; інформаційні системи (Інтернет-ресурси, цифровий репозиторій НУВГП, курс дисципліни на платформі Moodle); літературні джерела - підручники, посібники, методичні вказівки.
РН2. Вміти знаходити та обчислювати рівні побічних електромагнітних випромінювань на об’єктах інформаційної діяльності.	
Види навчальної роботи студента	Вивчення лекційного матеріалу (тема 2); самостійна робота з літературою; підготовка до контрольних заходів, виконання та захист лабораторної роботи № 1
Методи та технології навчання	Словесний метод; діалогічний метод; наочний метод; практичний метод; неімітаційні та імітаційні (неігрові) технології; інтерактивні технології (контекстне навчання; навчання на основі досвіду).
Засоби навчання	Комп'ютерна техніка; інформаційні системи (Інтернет-ресурси, цифровий репозиторій НУВГП, курс дисципліни на платформі Moodle); літературні джерела - підручники, посібники, методичні вказівки, спеціалізоване обладнання для пошуку побічних електромагнітних випромінювань, спеціалізоване програмне забезпечення для створення тестових сигналів.
РН3. Вміти локалізовувати небезпечні сигнали побічних електромагнітних випромінювань на об’єктах інформаційної діяльності.	
Види навчальної роботи	Вивчення лекційного матеріалу (тема 3); самостійна робота з літературою; підготовка до контрольних заходів, виконання та захист лабораторної роботи № 2
Методи та технології навчання	Словесний метод; діалогічний метод; наочний метод; практичний метод; неімітаційні та імітаційні (неігрові) технології; інтерактивні технології (контекстне навчання; навчання на основі досвіду).
Засоби навчання	Комп'ютерна техніка; інформаційні системи (Інтернет-ресурси, цифровий репозиторій НУВГП, курс дисципліни на платформі Moodle); літературні джерела - підручники, посібники, методичні вказівки, спеціалізоване обладнання для пошуку побічних електромагнітних випромінювань, спеціалізоване програмне забезпечення для створення тестових сигналів, спеціалізоване обладнання для створення шипокосмугового електромагнітного шумового сигналу.
РН4. Знати порядок застосування первинних та основних технічних засобів захисту від технічних каналів витоку інформації	
Види	Вивчення лекційного матеріалу (тема 4); самостійна

навчальної роботи студента	робота з літературою; підготовка до контрольних заходів, виконання та захист лабораторної роботи № 3
Методи та технології навчання	Словесний метод; діалогічний метод; наочний метод; практичний метод; неімітаційні та імітаційні (неігрові) технології; інтерактивні технології (контекстне навчання; навчання на основі досвіду).
Засоби навчання	Комп'ютерна техніка; інформаційні системи (Інтернет-ресурси, цифровий репозиторій НУВГП, курс дисципліни на платформі Moodle); літературні джерела - підручники, посібники, методичні вказівки, нормативні документи із технічного захисту інформації
РН5. Володіти основними поняттями політик безпеки операційних систем Windows та Linux	
Види навчальної роботи студента	Вивчення лекційного матеріалу (тема 5); самостійна робота з літературою; підготовка до контрольних заходів, виконання та захист лабораторної роботи № 4
Методи та технології навчання	Словесний метод; діалогічний метод; наочний метод; практичний метод; неімітаційні та імітаційні (неігрові) технології; інтерактивні технології (контекстне навчання; навчання на основі досвіду).
Засоби навчання	Комп'ютерна техніка; інформаційні системи (Інтернет-ресурси, цифровий репозиторій НУВГП, курс дисципліни на платформі Moodle); літературні джерела - підручники, посібники, методичні вказівки.
РН6. Оперувати основними функціями комплексів засобів захисту в автоматизованих системах від несанкціонованого доступу	
Види навчальної роботи студента	Вивчення лекційного матеріалу (тема 6); самостійна робота з літературою; підготовка до контрольних заходів, виконання та захист лабораторних роботи №№ 5-9
Методи та технології навчання	Словесний метод; діалогічний метод; наочний метод; практичний метод; неімітаційні та імітаційні (неігрові) технології; інтерактивні технології (контекстне навчання; навчання на основі досвіду).
Засоби навчання	Комп'ютерна техніка; інформаційні системи (Інтернет-ресурси, цифровий репозиторій НУВГП, курс дисципліни на платформі Moodle); літературні джерела - підручники, посібники, методичні вказівки, спеціалізоване програмне забезпечення «комплекс засобів захисту».
РН7. Володіти основними поняттями симетричних криптоалгоритмів та вимогами до криптографічних систем	
Види	Вивчення лекційного матеріалу (тема 7); самостійна

навчальної роботи студента	робота з літературою; підготовка до контрольних заходів, виконання та захист лабораторної роботи № 10.
Методи та технології навчання	Словесний метод; діалогічний метод; наочний метод; практичний метод; неімітаційні та імітаційні (неігрові) технології; інтерактивні технології (контекстне навчання; навчання на основі досвіду).
Засоби навчання	Комп'ютерна техніка; інформаційні системи (Інтернет-ресурси, цифровий репозиторій НУВГП, курс дисципліни на платформі Moodle); літературні джерела - підручники, посібники, методичні вказівки.
РН8. Володіти основними характеристиками алгоритмів мережі Фейстеля та криптоалгоритму DES	
Види навчальної роботи студента	Вивчення лекційного матеріалу (тема 8); самостійна робота з літературою; підготовка до контрольних заходів.
Методи та технології навчання	Словесний метод; діалогічний метод; наочний метод; практичний метод; неімітаційні та імітаційні (неігрові) технології; інтерактивні технології (контекстне навчання; навчання на основі досвіду).
Засоби навчання	Комп'ютерна техніка; інформаційні системи (Інтернет-ресурси, цифровий репозиторій НУВГП, курс дисципліни на платформі Moodle); літературні джерела - підручники, посібники, методичні вказівки.
РН9. Володіти основними характеристиками криптоалгоритму ГОСТ 28147-89	
Види навчальної роботи студента	Вивчення лекційного матеріалу (тема 9); самостійна робота з літературою; підготовка до контрольних заходів.
Методи та технології навчання	Словесний метод; діалогічний метод; наочний метод; практичний метод; неімітаційні та імітаційні (неігрові) технології; інтерактивні технології (контекстне навчання; навчання на основі досвіду).
Засоби навчання	Комп'ютерна техніка; інформаційні системи (Інтернет-ресурси, цифровий репозиторій НУВГП, курс дисципліни на платформі Moodle); літературні джерела - підручники, посібники, методичні вказівки.
РН10. Володіти основними характеристиками асиметричних криптоалгоритмів, зокрема алгоритму Діффі-Хеллмана та криптоалгоритму RSA.	
Види навчальної	Вивчення лекційного матеріалу (тема 10); самостійна робота з літературою; підготовка до контрольних

роботи студента	заходів, виконання та захист лабораторних робіт №№ 11 – 13.
Методи та технології навчання	Словесний метод; діалогічний метод; наочний метод; практичний метод; неімітаційні та імітаційні (неігрові) технології; інтерактивні технології (контекстне навчання; навчання на основі досвіду).
Засоби навчання	Комп'ютерна техніка; інформаційні системи (Інтернет-ресурси, цифровий репозиторій НУВГП, курс дисципліни на платформі Moodle); літературні джерела - підручники, посібники, методичні вказівки.
РН11. Знати основні принципи функцій хешування та технологій електронного цифрового підпису.	
Види навчальної роботи студента	Вивчення лекційного матеріалу (тема 11); самостійна робота з літературою; підготовка до контрольних заходів.
Методи та технології навчання	Словесний метод; діалогічний метод; наочний метод; практичний метод; неімітаційні та імітаційні (неігрові) технології; інтерактивні технології (контекстне навчання; навчання на основі досвіду).
Засоби навчання	Комп'ютерна техніка; інформаційні системи (Інтернет-ресурси, цифровий репозиторій НУВГП, курс дисципліни на платформі Moodle); літературні джерела - підручники, посібники, методичні вказівки.
РН12. Знати основні принципи криптоаналізу.	
Види навчальної роботи студента	Вивчення лекційного матеріалу (тема 12); самостійна робота з літературою; підготовка до контрольних заходів.
Методи та технології навчання	Словесний метод; діалогічний метод; наочний метод; практичний метод; неімітаційні та імітаційні (неігрові) технології; інтерактивні технології (контекстне навчання; навчання на основі досвіду).
Засоби навчання	Комп'ютерна техніка; інформаційні системи (Інтернет-ресурси, цифровий репозиторій НУВГП, курс дисципліни на платформі Moodle); літературні джерела - підручники, посібники, методичні вказівки.
РН13. Володіти основними засобами захисту комп’ютерих мереж.	
Види навчальної роботи студента	Вивчення лекційного матеріалу (тема 13); самостійна робота з літературою; підготовка до контрольних заходів.
Методи та технології	Словесний метод; діалогічний метод; наочний метод; практичний метод; неімітаційні та імітаційні (неігрові)

навчання	технології; інтерактивні технології (контекстне навчання; навчання на основі досвіду).
Засоби навчання	Комп'ютерна техніка; інформаційні системи (Інтернет-ресурси, цифровий репозиторій НУВГП, курс дисципліни на платформі Moodle); літературні джерела - підручники, посібники, методичні вказівки.

ЛЕКЦІЇ ТА ПРАКТИЧНІ РОБОТИ:

Тема 1. Поняття інформації. Загрози для інформації. Основні види технічних засобів розвідки.

Результати навчання:	Кількість годин:	Література:	Лінк на Moodle:
РН1	2 год лекцій; 9 год. сам. роб.	1, с.56-65; 2, с.21-25; 3, с. 69-75; 4, с.125-141; 5, с.123-147	https://exam.nuwm.edu.ua/course/view.php?id=3640

Опис теми:

Лекція 1. Поняття інформації. Загрози для інформації. Основні види технічних засобів розвідки.

Визначення інформації. Ідентифікація загроз для інформації. Класифікація основних форм розвідувальної діяльності. Види технічних засобів розвідки. Основні принципи добування інформації за допомогою технічних засобів

Сам. роб. Вивчення основних вимог щодо захисту від несанкціонованого доступу до інформації.

Тема 2. Технічні каналів витоку інформації. Класифікація. Види. Модель технічного каналу витоку інформації.

Результати навчання:	Кількість годин:	Література:	Лінк на Moodle:
РН2	2 год лекцій; 2 год. лаб. роб.; 9 год. сам. роб.	1, с. 131-147;	https://exam.nuwm.edu.ua/course/view.php?id=3640

Опис теми:

Лекція 2. Технічні каналів витоку інформації. Класифікація. Види. Модель технічного каналу витоку інформації.

Поняття технічного каналу витоку інформації. Класифікація ТКВІ. Небезпечні сигнали. Контрольована зона.

Лаб. роб. 1. Визначення амплітуди гармонік та побудова спектра побічних електромагнітних випромінювань монітора комп'ютера..

Сам. роб. Вивчення засобів та методів виявлення небезпечних сигналів на об’єктах інформаційної діяльності

Тема 3. Технічні канали витоку інформації. Побічні електромагнітні випромінювання.

Результати навчання:	Кількість годин:	Література:	Лінк на Moodle:
РН3	2 год лекцій; 2 год. лаб. роб.; 9 год. сам. роб.	1, с.78-98; 2, с.113-138.	https://exam.nuwm.edu.ua/course/view.php?id=3640

Опис теми:

Лекція 3. Технічні канали витоку інформації. Побічні електромагнітні випромінювання.

Фізичні основи побічних електромагнітних випромінювань. Рівняння

	Максвелла. Електрична та магнітна складові електромагнітного поля. Спектральна щільність випромінювання. **Лаб. роб. 2.** Створення широкосмугового сигналу завади для захисту від витоку за рахунок побічних електромагнітних випромінювань. **Сам. роб.** Вивчення природи утворення та розповсюдження електромагнітних випромінювань.

Тема 4. Технічні засоби захисту інформації. Захист інформації від технічних каналів витоку. Вимоги нормативних документів з питань технічного захисту інформації.			
Результати навчання: РН4	Кількість годин: 2 год лекцій; 2 год. лаб. роб.; 9 год. сам. роб.	Література: 1, с.115-173; 2, с.62-86; 3, с.19-34; 4, с.32-76;	Лінк на Moodle: https://exam.nuwm.edu.ua/course/view.php?id=3640
Опис теми:	**Лекція 4.** Технічні засоби захисту інформації. Захист інформації від технічних каналів витоку. Вимоги нормативних документів з питань технічного захисту інформації. *Локалізація побічних електромагнітних випромінювань. Захист від параметричних каналів витоку інформації.* **Лаб. роб. 3. Застосування положень** ТР ЕОТ – 95 в автоматизованих системах **Сам. роб.** Розробка плану захисту інформації на об'єкті інформаційної діяльності		

Тема 5. Програмні засоби захисту інформації. Підсистеми захисту в операційних системах.			
Результати навчання: РН5	Кількість годин: 2 год лекцій; 2 год. лаб. роб.; 9 год. сам. роб.	Література: 1, с.19-45; 3, с.138-153; 4, с.62-96.	Лінк на Moodle: https://exam.nuwm.edu.ua/course/view.php?id=3640
Опис теми:	**Лекція 5.** Програмні засоби захисту інформації. Підсистеми захисту в операційних системах. *Локальна підсистема безпеки. Журнал подій. Облікові записи. Диспетчер завдань. Ідентифікатор безпеки SID* **Лаб. роб. 4.** Дослідження політики облікових записів ОС WINDOWS **Сам. роб.** Вивчення політик безпеки операційної системи LINUX.		

Тема 6. Комплекси засобів захисту для автоматизованих систем.			
Результати навчання: РН6	Кількість годин: 2 год лекцій; 10 год. лаб. роб.; 9 год. сам. роб.	Література: 1, с.48-87; 3, с.408-463; 4, с.214-242; 5, с.179-207	Лінк на Moodle: https://exam.nuwm.edu.ua/course/view.php?id=3640
Опис теми:	**Лекція 6.** Комплекси засобів захисту для автоматизованих систем.		

	Функції комплексів засобів захисту. Функціональний профіль захищеності і рівень гарантій. Політики функціональних послуг безпеки. Монітор безпеки. **Лаб. роб. 5.** Вивчення основних функцій комплексу засобів захисту «Гриф-3». **Лаб. роб. 6.** Вивчення функціональних характеристик комплексу засобів захисту «Лоза-1». **Лаб. роб. 7.** Інсталяція та деінсталяція комплексу засобів захисту «Лоза-1» **Лаб. роб. 8.** Робота з переліком користувачів комплексу засобів захисту «Лоза-1» **Лаб. роб. 9.** Робота з переліком користувачів системи «Лоза-1» **Сам. роб.** Функціонал адміністратора КЗЗ та адміністратора безпеки комплексу засобів захисту від несанкціонованого доступу.
За поточну (практичну) складову оцінювання 36 балів	За модульний (теоретичний) контроль знань (МК1) 20 балів

Тема 7. Криптографічний захист інформації. Основні вимоги до криптографічних систем. Поняття криптоалгоритму. Симетричні криптоалгоритми			
Результати навчання: РН7	Кількість годин: 2 год лекцій; 2 год. лаб. роб.; 9 год. сам. роб.	Література: 1, с.188-204; 2, с.239-337; 3, с.243-307; 4, с.240-264	Лінк на Moodle: https://exam.nuwm.edu.ua/course/view.php?id=3640
Опис теми:	**Лекція 7.** Криптографічний захист інформації. Основні вимоги до криптографічних систем. Поняття криптоалгоритму *Історія криптології. Основні вимоги до криптосистем. Загальна схема симетричного шифрування. Методи заміни. Пропорційні шифри. Багатоалфавітна підстановки.* **Лаб. роб. 10.** Основи криптографічного захисту інформації. Симетричні криптоалгоритми**.** **Сам. роб.** Симетричні криптоалгоритми докомп'ютерного періоду		

Тема 8. Мережа Фейстеля. Криптоалгоритм DES			
Результати навчання: РН8	Кількість годин: 2 год лекцій; 9 год. сам. роб	Література: 1, с.205-234; 2, с.337-356; 3, с.308-317; 4, с.265-286	Лінк на Moodle: https://exam.nuwm.edu.ua/course/view.php?id=3640
Опис теми:	**Лекція 8.** Мережа Фейстеля. Криптоалгоритм DES *Вимоги до блокового криптоалгоритму. Алгоритм мережі Фейстеля. Криптоалгоритм DES – загальна схема, структура раунду.* **Сам. роб.** Симетричні криптоалгоритми на основі мережі Фейстеля.		

Тема 9. Криптоалгоритм ГОСТ 28147-89. Типові схеми. Структура раунду ГОСТ 28147-89. Алгоритми шифрування та розшифрування

Результати навчання: РН8	Кількість годин: 2 год лекцій; 4 год. сам. роб	Література: 1, с.235-254; 2, с.357-374.	Лінк на Moodle: https://exam.nuwm.edu.ua/course/view.php?id=3640

Опис теми:	**Лекція 9.** Криптоалгоритм ГОСТ 28147-89. Типові схеми. Структура раунду ГОСТ 28147-89. Алгоритми шифрування та розшифрування *Загальні відомості. Структура раунду. Процедури шифрування та розшифрування. Основні режими шифрування. Технології гамування та імітовставки.* **Сам. роб.** Застосування криптоалгоритму ГОСТ 28147-89 в для криптосистем різного рівня стійкості.

Тема 10. Асиметричні криптоалгоритми. Алгоритм Діффі-Хеллмана. Криптоалгоритм RSA. Основні відомості. Шифрування та розшифрування. Практичне використання

Результати навчання: РН8	Кількість годин: 2 год лекцій; 6 год. лаб. роб 4 год. сам. роб	Література: 1, с.255-282; 2, с.375-394;	Лінк на Moodle: https://exam.nuwm.edu.ua/course/view.php?id=3640

Опис теми:	**Лекція 10** Асиметричні криптоалгоритми. Алгоритм Діффі-Хеллмана. Криптоалгоритм RSA. Основні відомості. Шифрування та розшифрування. Практичне використання *Алгоритм Діффі-Хелмана - основні відомості, приклади обчислень, практичне використання. Криптоалгоритм RSA - основні відомості, приклади обчислень, практичне використання.* **Лаб. роб. 11** Генерація спільного закритого ключа для симетричного шифрування за алгоритмом Діффі-Хелмана **Лаб. роб. 12** Розрахунок параметрів відкритого та закритого ключа асиметричного криптоалгоритму RSA. Шифрування та розшифрування повідомлення за допомогою розрахованих параметрів. **Лаб. роб. 13** Шифрування інформації за допомогою асиметричних криптоалгоритмів в програмному середовищі Gpg4win **Сам. роб.** Асиметричні криптоалгоритми на еліптичних кривих

Тема 11. ХЕШ-функція. Електронний цифровий підпис.

Результати навчання: РН8	Кількість годин: 2 год лекцій; 4 год. сам. роб	Література: 1, с.284-325; 2, с.395-426;	Лінк на Moodle: https://exam.nuwm.edu.ua/course/view.php?id=3640

Опис теми:	**Лекція 11** ХЕШ-функція. Електронний цифровий підпис. *Алгоритми хешування. Застосування хеш-функцій. Хеш-функції сімейства MD. Електронний цифровий підпис.* **Сам. роб.** Хеш-функції сімейства SHA

Тема 12. Основні види атак, принципи криптоаналізу

Результати навчання: РН8	Кількість годин: 2 год лекцій; 4 год. сам. Роб	Література: 1, с.326-355; 2, с.427-448;	Лінк на Moodle: https://exam.nuwm.edu.ua/course/view.php?id=3640
Опис теми:	**Лекція 12** Основні види атак, принципи криптоаналізу *Класифікація атак на симетричні криптоалгоритми. Атака на основі шифротексту. Атака на основі обраного відкритого тексту. Атака на основі обраного шифротексту . Класифікація атак на асиметричні криптоалгоритми. Специфічний тип атаки "людина посередині". Атака на близькі значення p і q. Атака з вибраним шифротекстом.* **Сам. роб.** Криптоаналіз симетричних та асиметричних криптоалгоритмів		
Тема 13. Основи мережевої безпеки			
Результати навчання: РН8	Кількість годин: 2 год лекцій; 4 год. сам. Роб	Література: 4, с.214-275; 5, с.117-247;	Лінк на Moodle: https://exam.nuwm.edu.ua/course/view.php?id=3640
Опис теми:	**Лекція 13** Основи мережевої безпеки *Основні види атак на різних рівнях комп'ютерних мереж по моделі OSI.Загрози для IP-телефонії. Заходи мережевої безпеки. Захист у мережах Wi-Fi.* **Сам. роб.** Уразливості протоколів маршрутизації		

За поточну (практичну) складову оцінювання 24 бали	За модульний (теоретичний) контроль знань (МК2) 20 балів
Усього за поточну (практичну) складову оцінювання, балів	60
Усього за модульний контроль,або екзамен, балів	40
Усього за дисципліну, балів	100

Методи оцінювання та структура оцінки *COURSE GRADE COMPOSITION*	Для оцінювання рівня знань застосовується 100-бальна шкала оцінювання. Величина рівня засвоєння матеріалу навчання відбувається за такими методами: • поточне опитування після вивчення кожної теми; • оцінка за підготовку, виконання та захист лабораторної роботи; • оцінка за самостійну роботу; • підсумковий контроль у вигляді тестування: 2 модулі або екзамен. Основними показниками, що характеризують рівень знань студента за результатами вивчення дисципліни є: • виконання всіх видів навчальної роботи, що передбачені цим силабусом;

	• рівень знань навчального матеріалу за змістом навчальної дисципліни; • вміння студента презентувати свої знання, навички та отриманий практичний досвід; • вміння проводити аналіз результатів виконання лабораторних робіт та захищати одержані результати. Оцінювання результатів роботи проводиться у % від кількості балів, виділених на завдання, із заокругленням до цілого числа: 0% – завдання не виконано; 40% – завдання виконано частково та містить суттєві помилки методичного або розрахункового характеру; 60% – завдання виконано повністю, але містить суттєві помилки у розрахунках або в методиці; 80% – завдання виконано повністю і вчасно, проте містить окремі несуттєві недоліки; 100% – завдання виконано правильно, вчасно і без зауважень. ***Поточна (практична)*** складова оцінки (не більше, ніж 60 балів) нараховується за виконання лабораторних робіт (до 4 балів за кожну лабораторну роботу №№ 1 – 9, та по 6 балів за кожну лабораторну роботу №№ 10 – 13); виконання самостійної роботи (реферат, презентація – до 5 балів; виконання лабораторних робіт з програмною реалізацією – до 5 балів). ***Підсумкова (теоретична)*** складова оцінки курсу (не більше, ніж 40 балів) нараховується за модульний контроль (МК1 – до 20 балів; МК2 – до 20 балів) або за екзамен (ЕКЗ – до 40 балів). Модульні контролі та екзамен проводяться через ННЦНО НУВГП у формі комп'ютерного тестування на платформі Moodle. МК1, МК2 і ЕКЗ містять по 27 тестових завдань: 24 завдання першого рівня складності, 2 завдань другого рівня складності і 1 завдання третього рівня складності. За одне завдання першого рівня складності студент може отримати до 0,5 бала (МК1 і МК2) або 1 бал (ЕКЗ); за одне завдання другого рівня складності студент може отримати до 02 балів (МК1 і МК2) або до 4 балів (ЕКЗ); за одне завдання третього рівня складності – до 4 балів (МК1 і МК2) або до 8 балів (ЕКЗ).

	Додаткові бали (не більше, ніж 20): – за підготовку тез на наукову конференцію за тематикою навчальної дисципліни – до 10 балів; – за подання статті в збірник наукових праць – до 20 балів. ***Загальна інтегральна оцінка курсу*** розраховується як арифметична сума набраних балів (не більше, ніж 100) за всі види навчальних та додаткових завдань.
Місце навчальної дисципліни в освітній траєкторії здобувача вищої освіти	Опанування основними положеннями дисципліни передбачає наявність попередніх знань з вищої математики, математичної логіки та теорії алгоритмів, комп'ютерних мереж, операційних систем. Дисципліни, що вивчаються паралельно з цією: – Проектування інформаційних систем – Технології розподілених систем та паралельнихобчислень Дисципліни, для вивчення яких обов'язкові знання даної навчальної дисципліни: – Проектування інформаційних систем – Технології тестування програмних продуктів/ Моделювання систем
Інформаційні ресурси	**Рекомендована література** Основна 1. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средст-ва защиты информации . Том 1. Несанкционированное получение информации Киев: Арий 2008, 326с. 2. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средст-ва защиты информации . Том 2. Информционная безопасность Ки-ев: Арий 2008 385с. 3. Поповский В.В., Персиков А.В. Основы криптографической защиты информации в телекоммуникационных системах Харьков: СМИТ 2010 465с. 4. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем К, «ВНV», 2009. - 608с. 5.Бирюков И.В. Информационная безопасность. Защита и нападение : М, ДМК, 2017 - 434 с.

	Допоміжна 1. Мельников В. В. Защита информации в компьютерных системах. – М.: Финансы и статистика; Электронинформ, 1997.- 368с.:ил. 2. Шеннон К. Работы по теории информации и кибернетике, М., ИЛ, 1963, с. 333-369 (Перевод В.Ф.Писаренко) 3. Козлов Д. А., Парандовский А. А., Парандовский А. К. Энцикло-педия компьютерных вирусов. - М.: «СОЛОН-Р», 2001. 4. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита инфор-мации в компьютерных системах и сетях / Под ред. В. Ф. Шаньгина.-2-е изд., перераб. и доп.-М.: Радио и связь, 2001.-376 с: ил. 5. Фергюсон Н., Шнайер Б. Практическая криптография. : Пер. с англ. — М.: Издательский дом "Вильямс", 2005. — 424 с. : ил. 6. Хорошков В. А., Чекатков А. А. Методы и средства защиты ин-формации / Под ред. Ю. С. Ковтанюка – К.: Издательство Юниор, 2003.- 504с., ил. **7.** Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си. - М.: "Триумф", 2002. **Додаткові інформаційні ресурси** 1. Національна бібліотека ім. В. І. Вернадського. URL: http://www.nbuv.gov.ua/e-resources/, http://www.nbuv.gov.ua/webnavigator/ 2. Рівненська обласна універсальна наукова бібліотека (м. Рівне, майдан Короленка, 6). URL: http://www.libr.rv.ua/ 3. Рівненська централізована бібліотечна система (м. Рівне, вул. Київська, 44). URL: http://cbs.rv.ua/ 4. Наукова бібліотека НУВГП (м. Рівне, вул. Олекси Новака, 75). URL: http://nuwm.edu.ua/naukova-biblioteka/, http://nuwm.edu.ua/MySql/page_lib.php 5. Цифровий репозиторій НУВГП. URL: http://ep3.nuwm.edu.ua.

ПРАВИЛА ТА ВИМОГИ (ПОЛІТИКА)	
Дедлайни та перескладання	Завдання до лабораторних та самостійних робіт з відповідної теми повинні бути виконані і здані на оцінювання протягом 10 днів з дати заняття. При порушення термінів кількість балів знижується на 10%.

	Кінцевим терміном здачі завдань є останній робочий день навчального семестру (25 травня 2021 р.) Порядок повторного проходження контрольних заходів у НУВГП врегульовано «Положенням про семестровий поточний та підсумковий контроль навчальних досягнень здобувачів вищої освіти»: http://ep3.nuwm.edu.ua/5040/. Усі перездачі проходять за погодженням з директором ННІ. Правила ННЦНО стосовно повторного тестування наведено у документах: http://nuwm.edu.ua/strukturni-pidrozdili/navch-nauk-tsentr-nezalezhnoho-otsiniuvannia-znan/dokumenti. Перша перездача проводиться через ННЦНО згідно з розкладом перездач, який розміщено в додатку Мій НУВГП та ПС-Студент WEB: http://desk.nuwm.edu.ua/cgi-bin/shell.cgi?n=999. У випадку отримання незадовільної оцінки, здобувач направляється на комісію з перездачі дисципліни, яка формується деканатом ННІ. Після трьох невдалих спроб здачі семестрового підсумкового контролю з навчальної дисципліни вважається, що здобувач має академічну заборгованість. Рішення про повторне вивчення навчальної дисципліни або відрахування здобувача приймає ректор на підставі звернення директора ННІ, як це передбачено «Порядком ліквідації академічних заборгованостей у НУВГП»: http://ep3.nuwm.edu.ua/id/eprint/4273. У випадку нездачі підсумкового контролю через хворобу чи з інших поважних причин, здобувач має написати заяву на ім'я директора ННІ для зміни строків сесії.
Правила академічної доброчесності	Викладач та здобувачі несуть спільну відповідальність за створення сприятливого творчого навчального середовища, яке базується на взаємній повазі. До кожного заняття здобувачі повинні наперед ознайомитися з матеріалами та інформаційними ресурсами, наведеними у методичних вказівках і розміщеними на сторінці дисципліни в Moodle. Здобувачі освіти повинні дотримуватися Кодексу честі студентів. http://nuwm.edu.ua/strukturni-pidrozdili/vvrsdev/dokumenti Принцип студентоцентризму передбачає розуміння серйозності ставлення до академічної недоброчесності та неправомірної поведінки.

	Студенти мають самостійно виконувати і здавати на оцінювання лише результати власних зусиль та оригінальної праці. При виконанні практичних робіт з дисципліни студентам рекомендується працювати в навчальних групах, порівнювати отримані результати та обговорювати застосовувані методи. Однак виконуючи поставлені завдання, студенти повинні індивідуально здійснити кожен розрахунок. Обмін виконаними завданнями чи їх частинами у формі тексту, таблиці, програмного коду чи у будь-якій іншій формі є недопустимим. Не існує прийнятного приводу для плагіату чи обману. Здобувачі освіти не можуть копіювати виконані завдання у інших студентів, ділитися виконаними завданнями з іншими студентами і мають дотримуватися Положення про виявлення та запобігання академічного плагіату в НУВГП http://nuwm.edu.ua/sp/akademichna-dobrochesnistj У випадку плагіату при виконанні завдання здобувач не отримує бали і повинен виконати завдання повторно. Перевірка дотримання доброчесності під час модульного та підсумкового контролю може здійснюватися засобами відеонагляду. Здобувачі можуть робити аудіозапис аудиторного заняття для свого особистого освітнього використання тільки за погодженням з викладачем і не мають права розміщувати такий запис в соціальних мережах.
Вимоги до відвідування	Здобувачі вищої освіти зобов'язані відвідувати усі лекційні та практичні заняття з дисципліни згідно розкладу http://desk.nuwm.edu.ua/cgi-bin/timetable.cgi Відвідування консультацій не обов'язкове. У випадку відсутності з поважних причин (індивідуальний план, лікарняний, мобільність тощо) здобувач самостійно опрацьовує теоретичний матеріал і виконує завдання з відповідної практичної роботи. Завдання до практичних робіт розміщено на платформі Moodle https://exam.nuwm.edu.ua/course/view.php?id=1818 Файл (файли) із виконаними розрахунками здобувач прикріплює до відповідних завдань на платформі Moodle. Захист роботи відбувається на

	наступному занятті, консультації або онлайн у відеорежимі. На лекціях і практичних заняттях студенти можуть використовувати свої ноутбуки, планшети чи смартфони для роботи.
Неформальна та інформальна освіта	Визнання (перезарахування) результатів навчання, здобутих у неформальній та інформальній освіті, відбувається відповідно до «Положення про неформальну та інформальну освіту в НУВГП»: http://nuwm.edu.ua/sp/neformalna-osvita Здобувачі можуть пройти відкриті онлайн курси, близькі за темою до даної навчальної дисципліни, таких платформ як Coursera, Prometheus, edEx, edEra, VUMOnline, FutureLearn тощо. Зокрема, рекомендується курс на платформі Coursera: **Cybersecurity Compliance Framework & System Administration** https://www.coursera.org/learn/cybersecurity-compliance-framework-system-administration
ДОДАТКОВО	
Правила отримання зворотної інформації про дисципліну	Здобувач має право звертатися до викладача за додатковим поясненням матеріалу теми, змісту завдань практичних робіт та самостійної роботи протягом семестру усно (під час занять чи консультацій), корпоративною електронною поштою або через систему повідомлень Moodle. Консультації можуть проводитися онлайн із застосуванням сервісу Google Hangouts Meet. Здобувачі вищої освіти можуть подавати свої критичні зауваження, а також ідеї та рекомендації щодо наповнення навчальної дисципліни і методів викладання шляхом анонімного онлайн анкетування через Google Forms, яке проводиться наприкінці кожного семестру. Незалежне оцінювання якості викладання проводиться Відділом якості освіти. http://nuwm.edu.ua/strukturni-pidrozdili/vyo/dokumenti
Оновлення	Силабус переглядається кожного навчального року з урахуванням рекомендацій здобувачів освіти, які вони можуть подати під час онлайн опитування, з метою оновлення (осучаснення) змісту навчальної дисципліни на основі наукових досягнень і сучасних практик у галузі інформаційних технологій.
Навчання осіб з	Навчання людей з інвалідністю проводиться за

інвалідністю	дотриманням вимог нормативних документів, розроблених в НУВГП: http://nuwm.edu.ua/sp/dlja-osib-z-invalidnistju До здобувачів вищої освіти з особливими потребами є прохання: завчасно повідомити лектора про вказані особливості для відповідної підготовки та їх врахування в організації навчального процесу.
Інтернаціоналі-зація	Програма національних обмінів «Плацкарт» відповідно до Положення http://ep3.nuwm.edu.ua/13963/ . За угодами про міжнародну академічну мобільність (Еразмус+ К1), на основі двосторонніх договорів між НУВГП та зарубіжними навчальними закладами.

Лектор	**Назарук Віталій Дмитрович**, канд. техн. наук, ст. викладач кафедри обчислювальної техніки